

WHAT IS CLAIMED IS:

1. A system for enhancing the security of a computerized device, comprising:
a microprocessor-based Lockbox system in communication with the computerized device and through which all communications to the computerized device are routed through an internal firewall, a secure web server, with on-the-fly data encryption means for encryption of data between the computerized device and the Lockbox system allowing only encrypted data to be stored more than transitorily on the Lockbox system, and with on-the-fly decryption of the encrypted data; and
the data communication with the computerized device is possible only after passphrase enabling of the Lockbox from the computerized device and where the computerized device can disable this enabling until the next passphrase enabling.
2. The system of claim 1 wherein:
the computerized device is configured to segregate the encrypted data into client boxes and has the ability to designate some of that data for Internet communication; and
the Lockbox system is configured to provide an internet communication to the intended recipient informing the recipient of the availability of the data; and establish a secure socket communication with the recipient where, under passphrase access, the designated data can be copied by the recipient and files from the recipient can be received.
3. The system of claim 2 wherein the Lockbox is configured for secure time-stamped logging of the recipient-initiated communication of the data in a form that can only be altered by the computerized device for those logs before a predetermined time prior to the command.
4. The system of claim 2 wherein the Lockbox contains an application program to negotiate an encrypted communications over normal Internet communications with companion software on an external computer, with said application program having the ability to monitor the Lockbox data and exchange encrypted data with the companion

1007593-1-301
FOUO-632001

software to mirror the Lockbox data in the external computer and to maintain mirrored files as the Lockbox and external mirrored files are changed.

5. The system of claim 2 wherein the external computer companion software then having the ability to provide an internet communication to the intended recipient informing the recipient of the availability of the data; and establish a secure socket communication with the recipient where, under passphrase access, the designated data can be copied by the recipient and files from the recipient can be received and the function of backing up the Lockbox files.

6. A system for enhancing data integrity and security and facilitating secured network communications, the system comprising:

a dedicated processing system comprising a processor, memory, redundant non-volatile storage (fixed or removable), an Internet or local area network interface with a firewall and a local network interface; wherein the memory contains at least:

an operating system which can restrict the Internet access to the local network interface and restrict the downloading and running of applications not loaded at setup;

applications programs which, when executed by the processor, allow a computer on the local network interface to securely log onto the dedicated processing system to download and upload files to and from the non-volatile storage in a manner wherein the files are encrypted while stored on the non-volatile storage; and

applications programs which, when executed by the processor, are configured to insure files are archived redundantly and are able to be retrieved in the event of normal media failure or recent deletion.

7. A system as in claim 6 wherein selected file accesses, attempted system intrusions, system operating status and firewall transactions are time-stamped with a time referenced to a reliable source and recorded in encrypted form so that the record

1000789-11301

cannot be modified without extraordinary measures, and that a record is kept of all extraordinary measures.

8. A system as in claim 6 where a passphrase to unlock the system for system access may contain a letter from the month or day so as to cause the passphrase to be non-static so as to trigger a logged invalid system access.

9. A system as in claim 6 wherein the memory further contains an applications program configured to identify clients and associate files with those client accounts so that emails are automatically sent to the clients alerting them to the pending files in their accounts.

10. A system as in claim 9 wherein when the client accesses their account in response to a notification, access to that account is restricted by pass-phrase and the communication is secured by encryption.

11. A system as in claim 10 where by means of a tunneling mirror of the Lockbox files to a remote computer the remote computer can perform for the Lockbox the functions an internet communication to the intended recipient informing the recipient of the availability of the data; and establish a secure socket communication with the recipient where, under passphrase access, the designated data can be copied by the recipient and files from the recipient can be received and the function of backing up the Lockbox files.

12. A system as in claim 10 wherein when the client accesses his account and a selected file, that file is purged from the Lockbox.

13. A system as in claim 9 wherein the memory further contains an applications program configured to allow the client to acknowledge the file contents by a digital signature with the dedicated processor managing a PKI (Public Key Infrastructure) with no external access to the private key for the signature.

14. A system as in claim 13 wherein the PKI is managed to allow files transmitted over the Internet to be digitally signed with the private key inaccessible externally.

10007893, 111301